PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 :		(11) International Publication Number:
H04Q 7/00	A1	WO 92/02103
		(43) International Publication Date: 6 February 1992 (06.02.92)

(21) International Application Number: PCT/US91/04970

(22) International Filing Date: 15 July 1991 (15.07.91)

(30) Priority data:

554,951	16 July 1990 (16.07.90)	US
626,227	7 December 1990 (07.12.90)	US

(71) Applicant: MOTOROLA, INC. [US/US]; 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

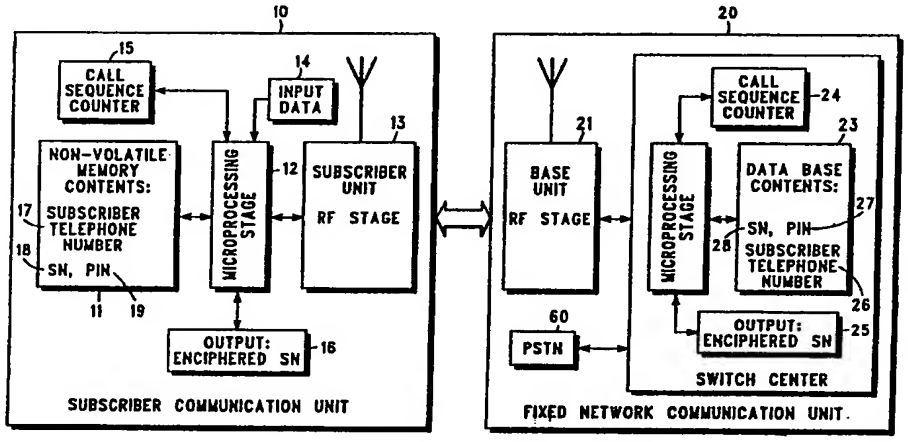
(72) Inventors: FLANDERS, Mary, Beth ; 108 Iroquois Trail, Wooddale, IL 60191 (US). FINKELSTEIN, Louis, D. ; 1698 W. Ottowa Court, Wheeling, IL 60090 (US). PUHL, Larry, C. ; 6 Plum Court, Sleepy Hollow, IL 60118 (US).

(74) Agents: PARMELEE, Steven, G. et al.; Motorola, Inc., Intellectual Property Dept., 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

(81) Designated States: CA, JP.

Published
With international search report.

(54) Title: METHOD FOR AUTHENTICATION AND PROTECTION OF SUBSCRIBERS IN TELECOMMUNICATION SYSTEMS



(57) Abstract

Radio frequency based cellular telecommunication systems often require a subscriber (10) to maintain a proprietary identifier (19) or serial number (18) which is transmitted to a fixed network communication unit (20) to verify the authenticity of the subscriber (10). An enciphering and call sequencing method is provided which can decrease unauthorized detection of these proprietary ID's (18, 19). This method permits efficient roaming by allowing authentication variables for multiple calls to be sent from the "home" system (20) to the "visited" system and stored by the "visited" system for use with subsequent calls. Further, a method is provided which forces the authenticating mobile (10) to use information that only it has available to itself. Furthermore, a method is provided which allows continued encryption integrity during handoffs by maintaining a record of pseudo random events between a subscriber unit (10) and any source radio communication unit (20) (e.g., the number of handoffs that the subscriber (10) has undergone during a given conversation).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	ES	Spain	MG	Madagascar
AU	Australia	FI	Finland	ML	Mali
BB	Barbados	FR	France	MN	Mongolia
BE	Belgium	GA	Gabon	MR	Mauritania
BF	Burkina Faso	GB	United Kingdom	MW	Malawi
BG	Bulgaria	GN	Guinea	NL	Netherlands
BJ	Benin	GR	Greece	NO	Norway
BR	Brazil	HU	Hungary	PL	Poland
CA	Canada	IT	Italy	RO	Romania
CF	Central African Republic	JP	Japan	SD	Sudan
CG	Congo	KP	Democratic People's Republic of Korea	SE	Sweden
CH	Switzerland			SN	Senegal
CI	Côte d'Ivoire	KR	Republic of Korea	SU+	Soviet Union
CM	Cameroon	LI	Liechtenstein	TD	Chad
CS	Czechoslovakia	LK	Sri Lanka	TG	Togo
DE	Germany	LU	Luxembourg	US	United States of America
DK	Denmark	MC	Monaco		

+ **It is not yet known for which States of the former Soviet Union any designation of the Soviet Union has effect.**

METHOD FOR AUTHENTICATION AND PROTECTION OF SUBSCRIBERS IN TELECOMMUNICATION SYSTEMS.

TECHNICAL FIELD

This invention relates generally to communication systems and more particularly to radio frequency (RF) cellular telecommunication systems.

BACKGROUND OF THE INVENTION

Cellular radio telephone systems typically include subscriber units (such as mobile or portable units) which communicate with a fixed network communication unit via RF transmissions. A typical fixed communication network includes at least a base station and a switching center. The switching center a subscriber unit accesses may not be his "home" switching center. In this case, the subscriber unit is termed a roamer. The switching center he accessed (termed the "visited" switching center) will communicate with his "home" switching center via the public switched telephone network (PSTN). One responsibility of the fixed network communication unit is to grant use of the communication system to the subscriber unit after the requesting subscriber unit meets the authentication requirements of the system. In a typical cellular telephone communication system, each subscriber unit is assigned a telephone number (mobile

identification number) (MIN) and an identification number (or serial number) (SN) which uniquely identifies the subscriber to any fixed network communication unit. Each subscriber unit has a unique identification number that distinguishes it from other subscriber units. The fixed network communication unit has access to these identification numbers through a database. Often these numbers are used by the fixed network communication units to bill subscribers for the time the subscriber uses the system. In the case of a roaming subscriber unit, the "visited" switching center must communicate with the subscriber's "home" system database to authenticate and bill the subscriber unit. If this communication is required for each call a subscriber unit makes, significant call setup delays will occur. When the subscriber calls another unit, he enters the phone number he wishes to call. The dialed phone number becomes the data to be sent to the fixed network communication unit. Data may also include other information regarding a third communication unit such as a unit's location.

Detection of a legitimate subscriber's identification number may be accomplished by RF eavesdropping or by purposeful or inadvertent divulgence of the MIN/SN combination by the radio telephone installer. Once the subscriber's telephone number and identification number is known (stolen), a thief may reprogram another subscriber unit with the stolen identification number causing two or more subscriber units to have the same MIN/SN combination. Cellular radio telephone systems have authentication procedures to deny access to subscribers not having legitimate identification numbers, but do not have the capability to detect multiple users or effectively neutralize the effect of an installer leaking subscriber identification numbers. Therefore, the legitimate user is billed for both the thief's use and his own use.

Several authentication techniques are known. EIA-553 section 2.3 specifies that each subscriber shall have a MIN and a factory set SN. The telephone number which the subscriber is attempting to contact is the data that is transmitted by the subscriber to the fixed network communication unit. Authentication is granted by this system if the MIN and corresponding SN are found in the fixed network communication unit database. Unfortunately, EIA-553 does not require the encipherment of the MIN or SN before transmission to the fixed network communication unit thereby permitting direct RF detection of any MIN or SN. In addition, this technique

fails to provide protection against a thief that acquires a MIN/SN from an installer.

Another authentication technique is described in European cellular communication system recommendations generated by the Groupe Special Mobile (GSM); see sections: 02.09, 02.17, 03.20, and 12.03. This method additionally requires the subscriber to openly transmit a temporary mobile subscriber ID (TMSI) to the fixed network communication unit; the fixed network communication unit generates and sends a random number (RAND) to the subscriber. The enciphering technique requires the subscriber unit to autonomously retrieve at least three enciphering elements from its memory: a predetermined ciphering key, an SN (individual subscriber authentication key) and a MIN (international mobile subscriber identification number - IMSI). The subscriber then enciphers its SN and MIN using the cipher to construct the RAND into a signed response (SRES). The subscriber unit transmits this signed response back to the fixed network communication unit where the fixed network communication unit checks the SN, MIN, and ciphering key against its database using the subscriber's temporary ID (TMSI).

The fixed network communication unit generates its response to the same random number using the information retrieved from the database and compares the subscriber signed response to the fixed network communication unit generated response. If the responses are substantially equivalent, authentication is confirmed. The dialed telephone number is only allowed to be transmitted after authentication is granted. This system affords some protection against a thief that acquires the MIN/SN from an installer by enciphering the SN and reassigning a temporary TMSI each time the subscriber enters a different cell area.

Although one technique enciphers the subscriber's serial number before transmission, neither system detects multiple users. Detection of thieves once they acquire access is important to maintaining a secure system. Moreover, the random number transmission (required for encipherment) necessitates additional communication between the subscriber unit and the fixed network communication unit each time a call is made which increases the probability of transmission error and adds a transmission step to the fixed network communication unit's authentication protocol routine. In addition, authentication must be verified before the

system will allow data to be accepted. Therefore data must be sent after the steps of the authentication procedure are complete.

Secure cellular systems also offer protection of conversations after authentication is granted. As is typical for cellular systems, the process of handing off a subscriber unit to another channel is needed for various reasons. These include maintaining communication link quality, minimizing co-channel interference between subscriber units, and managing traffic distributions. A handoff involves the transfer of communication between channels. Channelization may be in the form of time slots, frequencies, codes (as in spread spectrum type systems) and various combinations of these medium divisions. Handoffs include intracell handoffs, intercell handoffs, and intercluster handoffs. Intracell handoffs are those transfers between channels (voice or data) in the same cell; intercell handoffs are those transfers between channels in different cells, and intercluster handoffs are those transfers between channels in cells parented from different cell control units. In secure cellular systems wherein voice and/or data information is encrypted to avoid unauthorized detection of such information, handoffs introduce additional complications to maintaining encryption integrity.

In systems where absolute frame synchronization between base sites is not required, such as the proposed TDMA U.S. Digital Cellular system, subscriber units are only told which slots within a frame they must synchronize to after they are handed off. In a secure system however, voice encryption between the subscriber unit and any source basesite transceiver, typically requires an agreed starting point and must continue through the length of the call irrespective of the number of handoffs. At handoff, a conversation is already in progress, therefore lengthy gaps required to establish encryption synchronization must be avoided. Also, an intruder monitoring the channel at any point in the conversation should not be able to gain sufficient information to aid in any cryptanalysis effort.

One solution involves operating the encryption algorithm with a common mask that is reused for each slot of speech. However, this severely compromises the security of the encryption process since the same crypto-mask is repeated for each time slot thereby affording an intruder repeated chances for analyzing the same encyption process and consequently increasing the probability of decryption. At handoff this involves passing this mask from the source basesite (current serving

basesite to the target basesite. This allows the encryption process to remain synchronized to the handoff channel. Also, since the speech coder continues to generate it's output sequence during pauses in the conversation (quiet periods) an intruder has a good chance of determining the encryption process during these pauses.

Another solution involves restarting the encryption process at each handoff. However, this requires the repetition of the exact cipher stream after each handoff. An intruder's probability of decoding the cipher stream each time a handoff occurs is greatly increased; particularly in microcellular systems. The method of encryption must allow for a high degree of variability to make decryption more difficult. As during the authentication process, any variable used in the encryption process should not be communicated over the airwaves.

Another solution involves using a continuous stream encryption process wherein the process must maintain its continuity during all handoffs for the same conversation. For example, the exact starting point would have to be agreed upon by the subscriber unit and source basesite. At handoff, the current contents of the encryption process as well as the exact point of transfer is agreed upon by the source basesite and the target basesite. This method does not readily lend itself to a non-synchronous system since the target site may not know the current stage of the encryption process. Also, the length of messages between basesites would increase since a large number of memory elements may be needed to define the history of the encryption algorithm as started by the subscriber unit so that the target site can generate the current state of the encryption process.

There exists a need for a substantially enhanced authentication technique for a cellular telecommunication system that detects fraudulent users and efficiently protects identification numbers from unauthorized detection. This technique should permit roamers to access "visited" systems in an efficient and timely manner, while enabling the "visited" system to determine the legitimacy of the subscriber unit. The authentication method should restrict an illegitimate user's capacity to utilize the system in the case where access is inadvertently granted. Further, an adequate level of security resulting from encipherment should not require additional transmission processes or inject higher error levels during the authentication process: There also exists a need for an

encryption process for use in a synchronous channel or a non-synchronous channel system that provides encryption integrity during handoffs between channels such that an intruder is substantially prevented from decoding the encryption process.

BRIEF SUMMARY OF THE INVENTION

These needs and others are substantially met through provision of the method for authentication and protection of subscribers in telecommunication systems disclosed below. This method describes an authentication technique for use between a first communication unit, such as a subscriber unit, and a second communication unit, such as a fixed network communication unit, wherein the first communication unit modifies an ID, known to both the first communication unit and the second communication unit (such as a serial number), using data as one enciphering key and a second ID (such as a Personal Identification Number - PIN) as a second enciphering key as well as a network issued random number (RAND) as a third enciphering key. An historic non-arbitrary value of predetermined communication events, such as a count of the number of telephone calls made by a subscriber or a count of the number of handoffs that have occurred for the subscriber unit, is maintained in both the first and second communication units. This value (count) is historic because it represents past telephone calls attributed to a communication unit, and it is non-arbitrary because this history of transactions (i.e., number of calls made) serves to identify an out-of-sync communication unit.

The first communication unit transmits (via RF signals) the modified ID and count to a second communication unit. The second communication unit compares the count maintained by the first communication unit to the count maintained by the second unit. A count discrepancy indicates a different number of calls on one unit indicating a multiple user whose count is out of sequence. The second communication unit performs the same enciphering method on the known serial number using the data received and a known second ID. The second communication unit compares the received modified serial number and the serial number generated by the fixed network communication unit to determine if the serial number is valid. The invention is designed to substantially decrease unauthorized use of a

first ID of a communication unit. The authentication method does not require the second ID to ever be transmitted by RF.

This invention provides a means for detecting multiple subscribers using the same serial numbers and telephone numbers. Moreover, if a multiple user copies the information transmitted and uses the same information to access the system, the multiple user will be limited to only calling the telephone number that is in the authentication message; not a telephone number of his own choice. This authentication invention also reduces authentication errors by making more efficient use of the data transmitted and a second ID, by using them as a part of the cipher; the enciphering means does not require an additional RAND stream to be sent by a fixed network communication unit to be used as the common enciphering base and thereby eliminates this additional transmission and therefore decreases the probability of errors. This authentication scheme permits efficient roaming by allowing authentication variables for multiple calls to be sent from the "home" system to the "visited" system. These authentication variables can be stored by the "visited" switching center and used on subsequent calls. This storing allows the "visited" switching center to authenticate all subsequent calls without requiring real-time communication to the "home" system and without the associated call setup delays. It is also essential to retain the subscriber's secret keys (PIN) in the "home" switching center and not share this private information with the "visited" switching centers.

A method of stealing cellular service is to flash from a fraudulent mobile and take over an existing call. This flash message would tell the fixed network that the legitimate user is making a third party call. One possible solution to this problem is for the fixed network to initiate an authentication procedure on the traffic channel. However, the fraudulent mobile can allow the legitimate mobile to complete the authentication process. Another solution to this problem is to force the authenticating mobile to use information that only it has available to itself. A particular embodiment to this solution would be to exclusive-or (XOR) the dialed digits of the flash message with the output of the authentication algorithm and then send this response to the fixed network for verification that the legitimate mobile is really making a third party call. In the above scenario, since only the fraudulent mobile has the dialed digits that it is sending, the

legitimate mobile cannot correctly authenticate the flash message. Thus the fixed network would not complete the call from the fraudulent mobile.

In a secure cellular communication system using an encryption process utilizing at least one encryption key for encrypting information communicated over a channel, the method for preserving encryption integrity during a handoff includes: also maintaining a record of pseudo random events associated with a subscriber unit, such as the number of handoffs the subscriber unit has undergone during a given conversation with any number of source radio communication units; communicating the record, such as over a landline medium to prevent detection by an intruder, to a target radio communication unit; and restarting another encryption process for the subscriber unit using the record as an encryption variable.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a typical subscriber communication unit and fixed network communication unit.

FIG. 2 is a flow chart of the identification enciphering method used by a subscriber communication unit.

FIG. 3 is a flow chart of the authentication method used by a fixed network communication unit in accordance with the invention.

FIG. 4 is a flow chart generally depicting the method of preserving encryption integrity during handoffs in accordance with the invention.

FIG. 5 is a diagram generally depicting the encryption elements in accordance with the invention.

FIG 6. is a flowchart of an alternative authentication method used by a fixed network communication unit.

FIG. 7 is a diagram depicting a method of stealing cellular communication service which is eliminated by the authentication method shown in FIG. 6.

BEST MODE OF OPERATION

FIG. 1 generally depicts a subscriber communication unit (10) such as a subscriber telephone and a fixed network communication unit (20) such as a cellular telephone basesite and switching center. The subscriber communication unit (10) is comprised of a microprocessing stage (12), a non-volatile memory unit (11), a radio frequency (RF) stage (13), all as well

understood in the art. Additional elements include a data input stage (14) such as a key entry pad on a telephone (to enter a telephone number - data), a subscriber call sequence counter (15), and an output from an enciphering stage referred to as the enciphered serial number (16).

Within the non-volatile memory unit (11) resides the serial number (18) (for the subscriber unit), the PIN (19), and the subscriber telephone number (17) (which can have, for example, characteristics of a Mobile Identification Number (MIN)). The PIN is a second ID known only to the subscriber unit and the fixed network unit. For example, it should not be available to an installer of the subscriber unit, it should only be available to a legitimate user of a subscriber unit and a fixed network communication unit database. The subscriber need only enter the PIN one time to activate it. The PIN may be changed by the subscriber, but the change must also be made known to the fixed network unit. These identifiers need not necessarily be numbers but may correspond to any attribute capable of being identified by the fixed network communications unit. An alternative embodiment, for example, in a cellular system, may include a stored look up table containing multiple sets of serial numbers, PIN's, and telephone numbers with each set of identifiers corresponding to a specific cellular area or fixed network communication unit.

The fixed network communication unit (20) includes a switching center which is comprised of a microprocessing stage (22), a database (23), and a link to a basesite radio frequency stage (21), all as well understood in the art. Additional elements include a fixed network unit call sequence counter (24) and an enciphered serial number generated by the fixed network unit (25). Additionally, the switching center has an interface to the Public Switched Telephone Network (PSTN) (60). The PSTN link can be used for "visited" switching center to "home" switching center communications as required for authentication and billing of roaming subscriber units.

The database includes information regarding the subscriber unit's: serial number (18), PIN (19), and subscriber telephone number(17); the information is a copy of these ID's. The serial number (18), PIN (19), and telephone number (17) of the subscriber communication unit (10) correspond to the serial number (28), PIN (27), and telephone number (26) as stored in the fixed network communication unit (20). Communication between the subscriber communication unit (10) and the fixed network

communication unit (20) is accomplished via RF transmissions between the two units in accordance with well understood cellular system techniques.

When authentication is required of the subscriber communication unit (10), the subscriber unit enciphers its serial number (18) and increments its call sequence counter (15). FIG. 2 depicts the method used by a subscriber communication unit to encipher its serial number before transmission to a fixed network communication unit during an authentication request (29). This method requires use of at least two enciphering keys. The subscriber unit obtains the called telephone number (data)(30) and obtains PIN (31) from memory and uses at least parts of these two components as the enciphering keys to encipher its serial number (32). Alternatively, the subscriber unit obtains the called telephone number (DATA), a network issued random number (RAND) (30), a current subscriber's system number (historical data) as well as PIN (31) and uses at least parts of these components as the enciphering keys for enciphering its serial number (32). If PIN and the called telephone number are comprised of bits, the parts of these keys to be used are the contents of the bits and the bit length of each key. For example, an enciphered serial number may have a different bit length than the unenciphered serial number, or unmodified first ID, depending on the contents of the PIN or the data. Varying the enciphered SN bit length may also be a function of another event known to both the subscriber and fixed network unit such as the time of day.

The algorithm to integrate the enciphering keys may be varied to accommodate various levels of security depending upon the requirement of the system. The final step prior to transmission of the Authentication Response Message is to logically transform the enciphered message using the telephone number (data). This transformation is essential in assuring that a "visited" switching center can use the stored authentication variables it received previously from the subscriber's "home" switching center. The authentication variables issued by the "home" system make no assumptions about the telephone number (data) that the subscriber will use. Thus the "visited" system can compute the ARM based on the authentication variables it received from the "home" system and the received telephone number (data). The subscriber identification enciphering method does not require authentication to be confirmed by the fixed network communication unit before data is transmitted. Combining

PIN with data adds the ability of the system to encipher a serial number into a complex code to an extent sufficient to substantially eliminate unauthorized detection by RF eavesdropping and unauthorized divulgence by installers.

The modified serial number (enciphered SN) becomes a component of the Authentication Request Message (ARM) (35) that is transmitted via RF (36) to the fixed network communication unit. Once encipherment is complete, the assigned telephone number is obtained (33) from memory. This number is not enciphered as part of the authentication procedure. This identifier is a component of the ARM (35) that informs the fixed network unit that the authentication request is coming from a valid subscriber unit.

The call sequence count is then obtained (34) and also used in the ARM (35). The call sequence count is updated (incremented or decremented) each time a predetermined event occurs such as when the authentication procedure is initiated or when a call is completed. The count may be maintained by the subscriber and fixed network unit using a rollover type counter such as a ring counter. This count is used by the fixed network communication unit as a means to count the number of calls made by each subscriber. Another suitable count to be used in conjunction with, or instead of, the call sequence count is the number of handoffs associated with the subscriber unit. Because a record of the number of calls made by each subscriber is maintained by both the subscriber unit and the fixed network communication unit, another subscriber trying to use the same serial number will be detected because it will not have made the exact same number of calls as the legitimate subscriber. The call sequence count information is communicated to the fixed network unit as one component of the Authentication Request Message. The ARM can be communicated in any acceptable format or in any number of stages. Components of a typical ARM (35) include data, the enciphered serial number, the call sequence count, and the assigned telephone number. An alternative embodiment would include modifying the call sequence count using the same enciphering method that is used to modify the SN. This would further enhance the protection because the count is also disguised using the PIN and data; each subscriber would generate a different value for the same count (number of calls made).

A fixed network communication unit receives a transmitted ARM and uses this information to determine whether authentication should be

granted to the subscriber unit. FIG. 3 depicts the authentication method performed by a fixed network unit. The ARM is received (37) by the fixed network unit by means of the base RF unit (21). The fixed network unit has access to assigned telephone number's, serial number's and PIN's of valid subscriber units through its database. The fixed network unit determines if the assigned telephone number received in the ARM is valid (39) by obtaining from the fixed network unit database the same assigned telephone number (38). A comparison is made between the received telephone number from the subscriber unit and the valid number found in the database (39). If the assigned telephone number is not recognized by the fixed network unit, authentication is denied (or some other action taken) (40).

If the assigned telephone number is determined to be valid (it is found in the database), the fixed network unit then retrieves from the database the serial number and PIN corresponding to that particular assigned telephone number. The fixed network unit then, uses the PIN from the database and the data received in the ARM as enciphering keys as elements of its enciphering method (44), which is the same method used in the subscriber unit, and generates its own enciphered serial number. The fixed network unit compares this enciphered serial number to the serial number enciphered by the subscriber unit(46). If they are not substantially the same, then the system denies access or takes some other predetermined course of action (47). If they are within the acceptable tolerance, the received call sequence count is obtained (48) and compared (50) to the call count maintained by the fixed network communication unit (49). If the counts are substantially equal, authentication may be confirmed (52) which is the first predetermined course of action. At this point, the subscriber may be allowed to communicate with the third communication unit associated with the dialed number. This third unit may more generally be termed a requested communication resource. If the count is not within the acceptable tolerance, authentication may be denied or the authorities may be notified that a multiple user is attempting to access the system (51).

The fixed network unit call counter maintains the number of times authentication is granted to a subscriber. Each subscriber has its own call counter. Having a continuous call counting scheme between a subscriber and a fixed network communication unit prevents another subscriber from

using some other subscriber's identification number because the thief would not have made the identical number of calls that the legitimate subscriber made. This discrepancy is flagged by the fixed network unit when it compares the two counts.

Protection against illegitimate users is further enhanced by the encipherment method's use of the enciphered dialed telephone number and the PIN (which is not transmitted). Without an illegitimate user knowing a subscriber's PIN and the exact algorithm that enciphers the serial number, a thief is limited to merely copying the authentication message of a subscriber and repeating this message. Each time a subscriber dials a different telephone number, a different authentication request message is generated because each subscriber has a different PIN; each subscriber generates a different authentication request message for the same telephone number.

Although a thief may detect the call sequence count (because it is not enciphered in the ARM) and update it, a correct count would only allow the thief to gain authentication for the enciphered dialed telephone number he intercepted. Therefore the illegitimate user can only communicate to the subscriber whose enciphered telephone number matches that copied from the ARM.

An alternative embodiment comprising the call sequence count may allow each subscriber to maintain more than one call counter where a separate call counter is required for each fixed network communication unit. This embodiment would find use in a cellular communication system which allowed a subscriber to use multiple fixed network communication units. Another alternative embodiment to the flow in FIG. 3 may require the step of comparing the call sequence counts (50) to occur before the step involving the comparison of enciphered serial numbers (46).

In FIG. 7, a method of stealing cellular service is shown. In particular, an illegitimate user (704) waits until a legitimate user (702) makes a valid call. The illegitimate user then overpowers the traffic channel between the legitimate user (702) and a base site (700) with a third party flash call. The illegitimate user (704) drops off of the traffic channel while the base site (700) sends an authentication request message to the legitimate user (702). The legitimate user (702) responds to the authentication request, correctly. Thus, the base site connects the third party call. Meanwhile, the illegitimate user (704) overpowers the

traffic channel and takes control. The original call between the legitimate user (702) and the base site (700) is lost and the legitimate user (702) drops out of the traffic channel. As a result, the illegitimate user (704) continues the call with the third party that was called and the filling for the call is sent to the legitimate user (702).

In FIG. 6, a method of eliminating this form of stealing cellular service is shown. This elimination is accomplished by requiring the authentication response message from a mobile unit to contain an exclusive-or of at least part of the response message with the dialed digits. Since the legitimate mobile unit does not know the illegitimate mobile units dialed digits, the legitimate mobile unit authenticates incorrectly and the third party call of the illegitimate mobile unit does not go through.

Referring now to FIG.2 and FIG. 6, in particular, FIG. 6 depicts an alternative authentication method used by a fixed network communication unit which supports authentication of roaming mobile units. In this embodiment an Authentication Request Message (ARM) is received from a subscriber communication unit (10) (mobile unit) by the fixed network unit (20) through a base unit RF stage (21). The ARM preferably includes a Mobile Identification Number (MIN), the Dialed Digits (Data) and a Call Sequence Count. From the received ARM the fixed network unit (20) determines whether the received ARM comes from a mobile in its home network (602).

If the received ARM is from a home mobile unit, then the fixed network unit (20) determines if the assigned MIN (preferably telephone number) in its database (23) is the same as the MIN received in the ARM (604). A comparison is made between the received MIN from the mobile unit (10) and the valid MIN found in the database (23). If the received MIN is not recognized by the fixed network unit (20), service is denied (or some other action is taken) (606). Otherwise, if the received MIN is determined to be valid (it is found in the database), then the fixed network unit (20) retrieves a Personal Identification Number (PIN) from the database (23) and generates a particular random/response pair (RAND/RESP) from this PIN (608). The RAND preferably is a random number and the RESP preferably is a number which is generated as a function of the RAND and the particular subscriber's PIN. In alternative embodiments it will be appreciate that the RESP may be generated as a function of additional

elements such as a MIN, Electronic Serial Number, and/or rolling key. Subsequently, the authentication method continues at step (622).

Otherwise, if the received ARM is not from a home mobile, then the fixed network (20) checks its database (23) for RAND/RESP pairs for this visiting mobile unit (610). If the database (23) contains RAND/RESP pairs for this visiting mobile unit, then the fixed network (20) retrieves a particular RAND/RESP pair for use in this particular authentication process (612) and continues the authentication process at step (622). Otherwise, if the fixed network unit's database (23) does not contain RAND/RESP pairs for this visiting mobile unit, the fixed network unit (20) preferably accesses the visiting mobile unit's home network via a PSTN link (60). The home network determines if the assigned MIN (preferably telephone number) in its database is the same as the MIN received in the ARM (614). A comparison is made between the received MIN from the visiting mobile unit and the valid MIN found in the home network's database. If the received MIN is not recognized by the home network, service is denied (or some other action is taken) (616). Otherwise, if the received MIN is determined to be valid (it is found in the database), then the home network provides RAND/RESP pairs for this visiting mobile unit to the visited network unit (20) preferably via the PSTN link (60) (618). The fixed network unit (20) stores these received RAND/RESP pairs in database (23) (620). Subsequently, the fixed network (20) retrieves a particular RAND/RESP pair for use in this particular authentication process (612) and continues the authentication process at step (622).

At authentication step (622), the fixed network unit (20) generates a $RESP_D$ which is a logical function of the RESP associated with the particular RAND for this authentication process and the Dialed Digits received in the ARM (preferably an XOR function or other non-destructive logical function). Subsequently, the fixed network unit (20) issues the particular RAND to the mobile unit (10) (624). The mobile unit (10) generates a RESP from this particular RAND using a particular method which is the same method as the one used by the network unit (either home or visited network unit). Then, the mobile unit (10) generates a $RESP_D$ which is a logical function of the mobile generated RESP and the Dialed Digits sent in the ARM (preferably an XOR function or other non-destructive logical function) and provides the mobile generated $RESP_D$ to the fixed network unit (626). The fixed network unit (20) compares this

received $RESP_D$ to the network unit generated $RESP_D$ (628). If they are not substantially similar, then service is denied (or some other action is taken) (630).

Otherwise, if the two $RESP_D$'s are substantially similar, then the Call Sequence Count received in the ARM is compared to the Call Sequence Count maintained by the fixed network unit (10) (632). If the counts are not within an acceptable tolerance, then the service is denied, the authorities may be notified that a multiple user is attempting to access the system (634) and/or some other appropriate action is taken. Otherwise, if the counts are substantially equal, authentication may be confirmed and service issued (636). At this point, the mobile unit (10) may be allowed to communicate with the third communication unit associated with the Dialed Digits received in the ARM and the authentication process is done (638).

Figure 4 begins with block 400 wherein the source basesite is currently using a first encryption process to secure the traffic channel over which speech is being communicated between the subscriber unit and the source station. Once a handoff is required (405) both the subscriber unit and neighboring base sites are used in determining the proper target site using well known cell selection techniques. After the proper channel and target site are identified, the current handoff count and the session key are communicated over the landline network to the target site (410). The subscriber unit is given the new handoff channel over which it will communicate with the target unit (415). The subscriber unit and target site then modify their handoff count registers (420).

The target site will broadcast a frame count over an RF link to the subscriber unit for a short period of time after a channel has been assigned (425). The target basesite will cease the broadcast once the subscriber unit has acquired the correct frame count. The handoff count is therefore maintained by the subscriber unit and source basesite, updated for each handoff, and is typically unique for each call. The combination of the handoff count and the frame count serves as a pseudo-secret crypto-sync variable. The target site continues communication with the subscriber unit on the target channel by restarting the encryption process using the received handoff count as a new encryption variable (430).

As appreciated by those of ordinary skill in the art, the target unit and the source unit may be the same communication unit as in the case of a channel handoff between time slots from the same carrier frequency or a

transfer to another code in the same time slot as in a code division multiplexed system.

This method of preserving encryption integrity uses a substantially random variable as a new encryption variable for the time slot from which the target site continues communication each time a handoff occurs. It also forces the encryption process to start again after each handoff thereby not requiring continuous encryption process synchronization between voice coders from differing sites or channels. Such an encryption scheme uses the pseudo random events of handoffs associated with a subscriber unit, such as between subscribers and various channels, to ensure adequate protection from unauthorized listeners. The degree of randomness of the number of handoffs that may occur during any given conversation depends on such factors as cell size, propagation medium characteristics, receiver sensitivities of the subscriber unit and base sites, handoff thresholds as set by the system operator, and various other factors. Consequently, the handoff count in microcellular systems and in-building systems may vary substantially more than a rural system having large cells. Unlike these pseudo random events, predictable events such as the time of day or absolute frame number (as in a synchronous TDMA system), do represent adequate encryption variables since they do not offer same degree of randomness. The intruder can readily predict an amount of elapsed time since the last call or handoff or can readily determine the absolute frame number since it is generally broadcast over the RF medium. In the case of a synchronous TDMA system, the target site may determine proper frame count synchronization from the switch, source site, or other suitable means.

FIG. 5 shows an bit map for a typical initialization vector (500) and key field (505) for carrying out the method of preserving encryption integrity during handoffs. The encryption key field is termed the session key field since it is unique for each session or call and changes on a per call basis. The initialization vector (500) includes the pseudo random encyption variable and is maintained by both the subscriber unit and the basesite and changes for each slot. The initialization vector (500) contains 32 bits and these 32 bits are combined with the session crypto-key (505) to produce 159 bits needed for each slot. The 32 bits are divided between three counters: an eight bit handoff counter, a nine bit speech slot counter, and a fifteen bit speech slot overflow counter. The handoff counter is updated as previously described. The slot counter is given the slot count of the target

unit and overflow counter is started from a count of zero at the beginning of a call and at every handoff thereafter. The basesite establishes synchronization with the subscriber unit by sending, via RF, the nine bits of the slot counter during every slot, for a predetermined time, at the beginning of its transmission until the target site correctly decrypts speech, which may be generated using VSELP coding or other suitable speech coding method, from the subscriber unit or until the predetermined time elapses.

The session key field in combination with the initialization vector are used in an encryption algorithm (510) to generate an output mask (515) which is exclusive ORed (518) with the speech (520) or data. This output is then further error coded using known error protection techniques (525).

The session key and the handoff counts are communicated over the landline network between base sites to prevent detection by RF intruders. Since the subscriber itself maintains a handoff count and the fixed network also maintains the count, there is no need to broadcast this information over an RF channel thereby keeping the handoff count a pseudo-secret crypto-variable.

The above method provides synchronization for speech encryption in a system that does not have an absolute frame synchronization scheme between base sites. However, as obvious to those of ordinary skill in the art, the method for preserving encryption integrity during handoff may be readily applied to any suitable secure cellular system. Although a count of channel handoffs is the preferred pseudo random event, other suitable pseudo random events may also be used including the number of calls made by a given subscriber unit, or the number of power changes a subscriber unit undergoes. As appreciated by those skilled in the art, a record of pseudo random events may include other representations of the events other than a count of such events. Maintaining a count is only one way of representing events.

As appreciated by those skilled in the art, numerous alternative embodiments may be devised without departing from the spirit and scope of the claimed invention.

CLAIMS

What is claimed is:

1. In a telecommunication system using an encryption process, a method of subscriber protection comprising:
   (a) maintaining a record of pseudo random events associated with a subscriber unit;
   (b) communicating the record to a target radio communication unit; and
   (c) utilizing another encryption process as between the subscriber unit and the target radio communication unit using the record as an encryption variable.

2. The method according to claim 1 wherein the record of pseudo random events comprises the record of a number of channel handoffs attributed to the subscriber unit.

3. A method of authentication and protection between a subscriber unit and a central communication unit in a radiotelephone communication system, comprising the steps of:

(a) providing the subscriber unit with a first ID and a terminal endpoint identifier which uniquely identifies a target communication unit other than the central communication unit;

(b) generating a modified first ID in the subscriber unit by modifying the first ID as a function of a random number received from the central communication unit;

(c) modifying the modified first ID in the subscriber unit as a function of the terminal endpoint identifier; and

(d) transmitting via a radio communication link the modified first ID from the subscriber unit to the central communication unit.

4. The method according to claim 3 wherein:

(a) the subscriber unit is provided with a second ID; and

(b) the modified first ID is generated in the subscriber unit by modifying the first ID as a function of the received random number and the second ID.

5. A method of authentication and protection between a subscriber unit and a central communication unit in a radiotelephone communication system, comprising the steps of:

(a) providing the central communication unit with information regarding a first ID;

(b) receiving a request for service at the central communication unit from the subscriber unit, the request for service comprising a terminal endpoint identifier which uniquely identifies a target communication unit other than the central communication unit;

(c) transmitting via a radio communication link a random number from the central communication unit to the subscriber unit in response to receiving the request for service;

(d) receiving a modified first ID at the central communication unit, the modified first ID being derived from the first ID, transmitted random number and the terminal endpoint identifier; and

(e) determining in the central communication unit, through the use of the received modified first ID, the received terminal endpoint identifier, the transmitted random number and the information regarding the first ID, if the received service request is authentic.

6. The method according to claim 5 wherein:

(a) the central communication unit is provided with a second ID; and

(b) the determining if the received service request is authentic further includes the use of the second ID.

7. The method according to claim 5 wherein:

(a) the central communication unit is a home communication unit for the subscriber unit; and

(b) the information regarding the first ID is substantially similar to the first ID.

8. The method according to claim 5 wherein:

(a) the central communication unit is a visited communication unit for the subscriber unit;

(b) the step of providing the central communication unit with information regarding a first ID, comprises the steps of:

(i) determining if the visited communication unit has information regarding the first ID;

(ii) retrieving the information regarding the first ID, if the visited communication unit has the information regarding the first ID; and

(iii) communicating with a home communication unit for the subscriber unit, subsequently retrieving the information regarding the first ID, and subsequently storing the information regarding the first ID in the visited communication unit, if the visited communication unit does not have the information regarding the first ID.

9. A method of authentication and protection between a subscriber unit and a central communication unit in a radiotelephone communication system, comprising the steps of:

(a) providing the subscriber unit with a first ID and a terminal endpoint identifier which uniquely identifies a target communication unit other than the central communication unit;

(b) providing the central communication unit with information regarding the first ID;

(c) transmitting via a radio communication link a request for service from the subscriber unit to the central unit, the request for service comprising the terminal endpoint identifier;

(d) receiving the request for service at the central communication unit;

(e) transmitting via a radio communication link a random number from the central communication unit to the subscriber unit;

(f) receiving the random number at the subscriber unit;

(g) generating a modified first ID in the subscriber unit by modifying the first ID as a function of the received random number;

(h) modifying the modified first ID in the subscriber unit as a function of the terminal endpoint identifier;

(i) transmitting via a radio communication link the modified first ID from the subscriber unit to the central communication unit;

(j) receiving the modified first ID at the central communication unit; and

(k) determining in the central communication unit, through the use of the received modified first ID, the received terminal endpoint identifier, the transmitted random number and the information regarding the first ID, if the received service request is authentic.

10. The method according to claim 9 wherein:

(a) the subscriber unit is provided with a second ID;

(b) the central communication unit is provided with the second ID;

(c) the modified first ID is generated in the subscriber unit by modifying the first ID as a function of the received random number and the second ID; and

(d) the determining if the received service request is authentic further includes the use of the second ID.

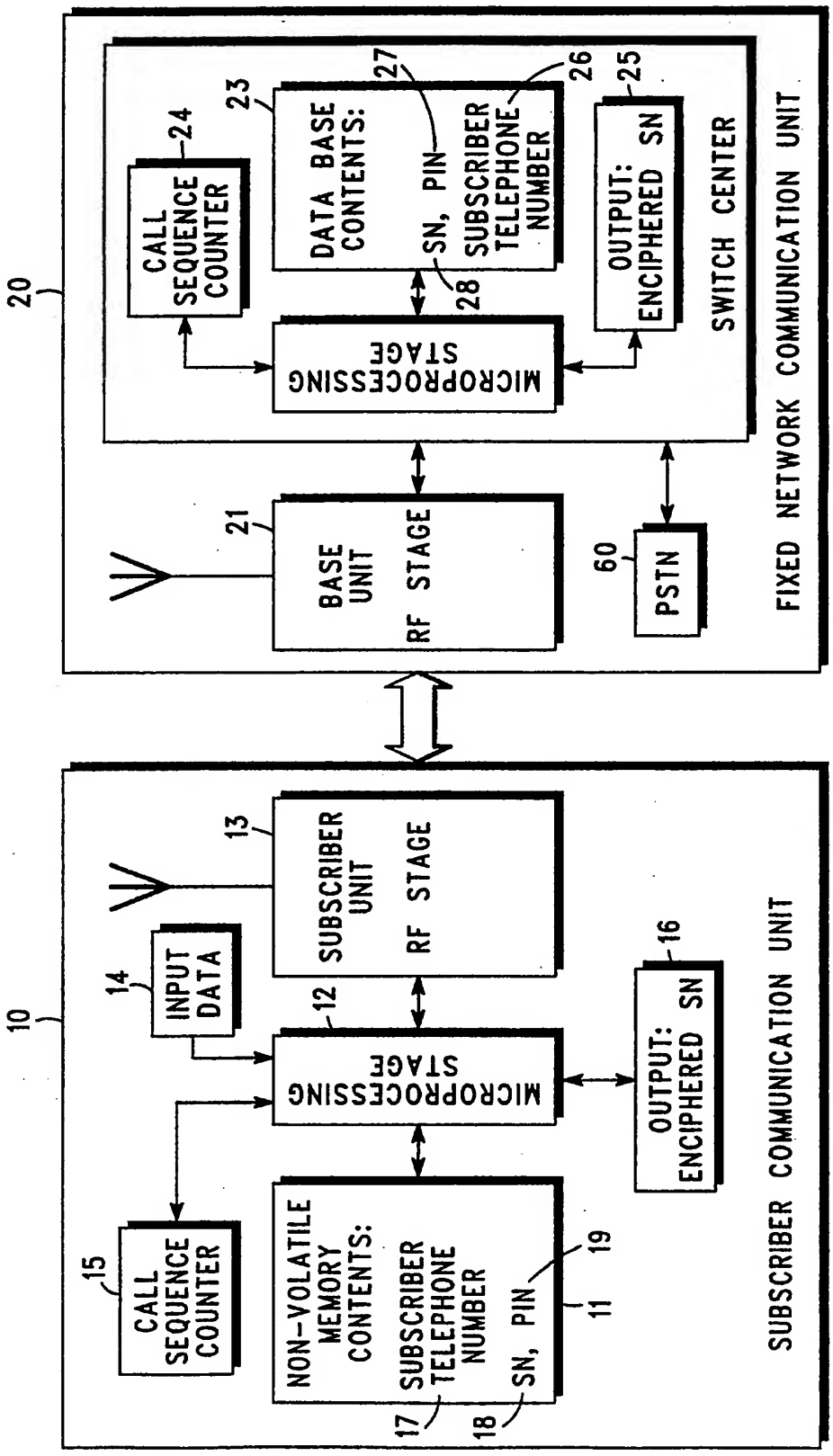

FIXED NETWORK COMMUNICATION UNIT
SWITCH CENTER
20
CALL SEQUENCE COUNTER
24
DATA BASE CONTENTS:
23
SN, PIN
27
SUBSCRIBER TELEPHONE NUMBER
26
OUTPUT: ENCIPHERED SN
25
28
MICROPROCESSING STAGE
BASE UNIT RF STAGE
21
PSTN
60
SUBSCRIBER COMMUNICATION UNIT
10
SUBSCRIBER UNIT RF STAGE
13
INPUT DATA
14
MICROPROCESSING STAGE
12
OUTPUT: ENCIPHERED SN
16
CALL SEQUENCE COUNTER
15
NON-VOLATILE MEMORY CONTENTS:
SUBSCRIBER TELEPHONE NUMBER
17
SN, PIN
18
19
11

FIG.1

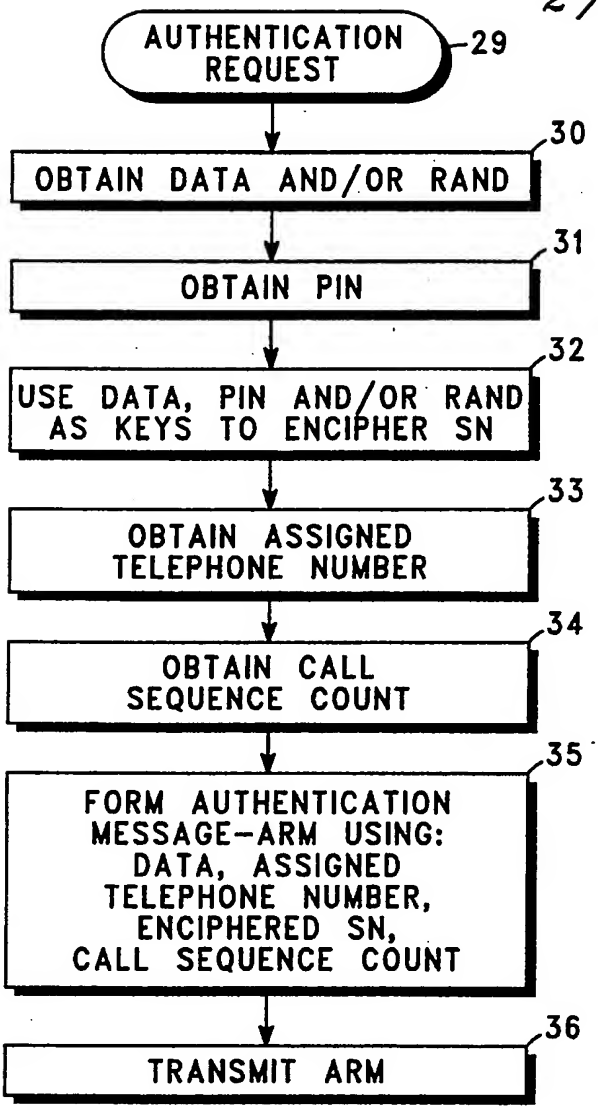

AUTHENTICATION REQUEST
29
OBTAIN DATA AND/OR RAND
30
OBTAIN PIN
31
USE DATA, PIN AND/OR RAND AS KEYS TO ENCIPHER SN
32
OBTAIN ASSIGNED TELEPHONE NUMBER
33
OBTAIN CALL SEQUENCE COUNT
34
FORM AUTHENTICATION MESSAGE-ARM USING: DATA, ASSIGNED TELEPHONE NUMBER, ENCIPHERED SN, CALL SEQUENCE COUNT
35
TRANSMIT ARM
36

FIG.2

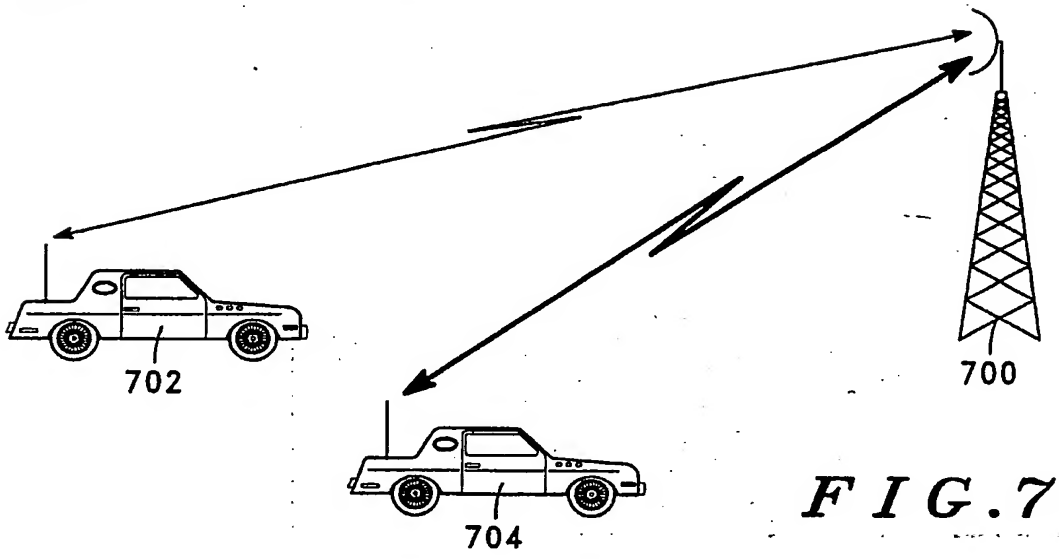

702
704
700

FIG.7

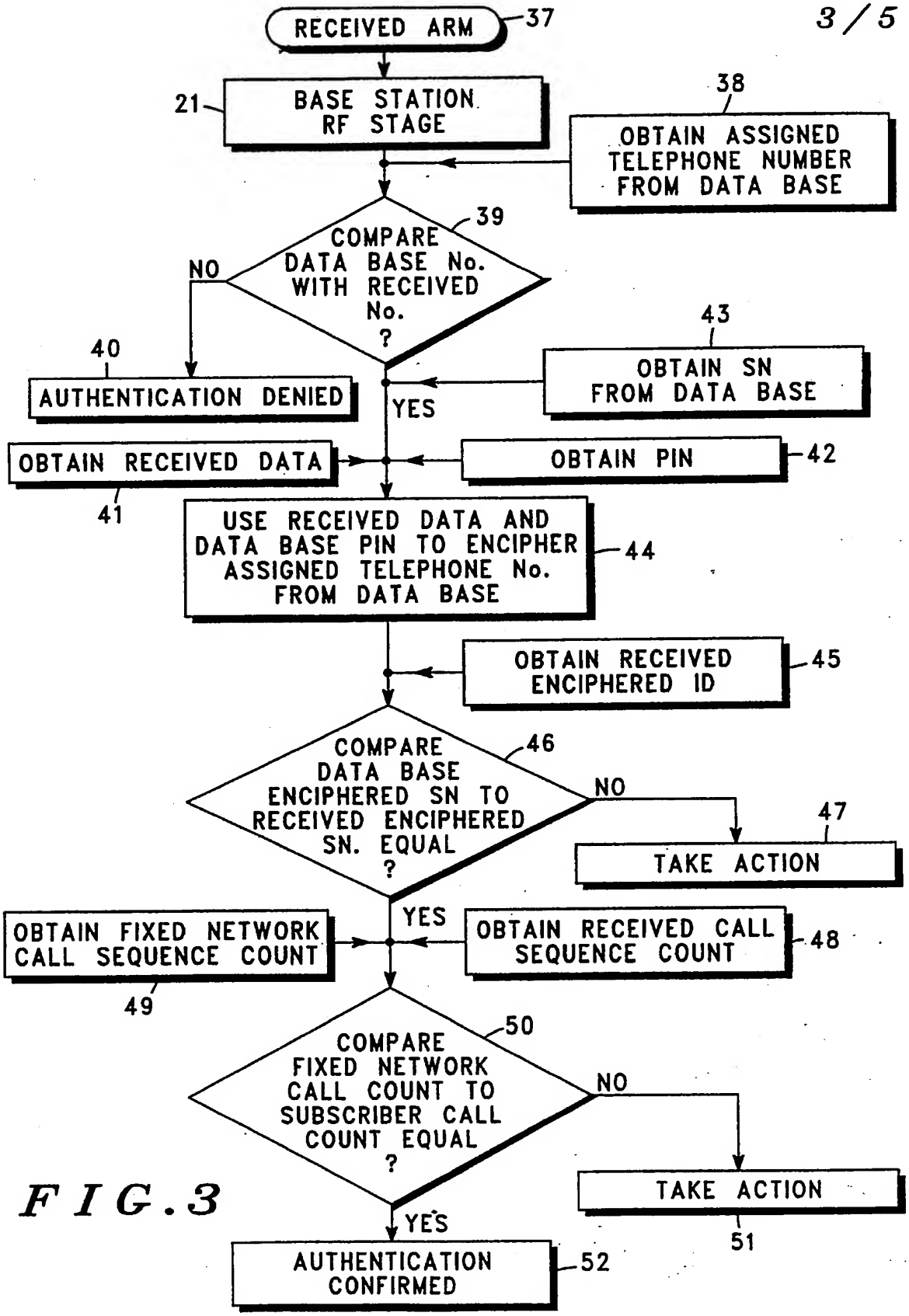

RECEIVED ARM
37
21
BASE STATION RF STAGE
38
OBTAIN ASSIGNED TELEPHONE NUMBER FROM DATA BASE
39
COMPARE DATA BASE No. WITH RECEIVED No. ?
NO
40
AUTHENTICATION DENIED
43
OBTAIN SN FROM DATA BASE
YES
OBTAIN RECEIVED DATA
41
OBTAIN PIN
42
USE RECEIVED DATA AND DATA BASE PIN TO ENCIPHER ASSIGNED TELEPHONE No. FROM DATA BASE
44
OBTAIN RECEIVED ENCIPHERED ID
45
COMPARE DATA BASE ENCIPHERED SN TO RECEIVED ENCIPHERED SN. EQUAL ?
46
NO
47
TAKE ACTION
YES
OBTAIN FIXED NETWORK CALL SEQUENCE COUNT
49
OBTAIN RECEIVED CALL SEQUENCE COUNT
48
COMPARE FIXED NETWORK CALL COUNT TO SUBSCRIBER CALL COUNT EQUAL ?
50
NO
TAKE ACTION
51
YES
AUTHENTICATION CONFIRMED
52

FIG. 3

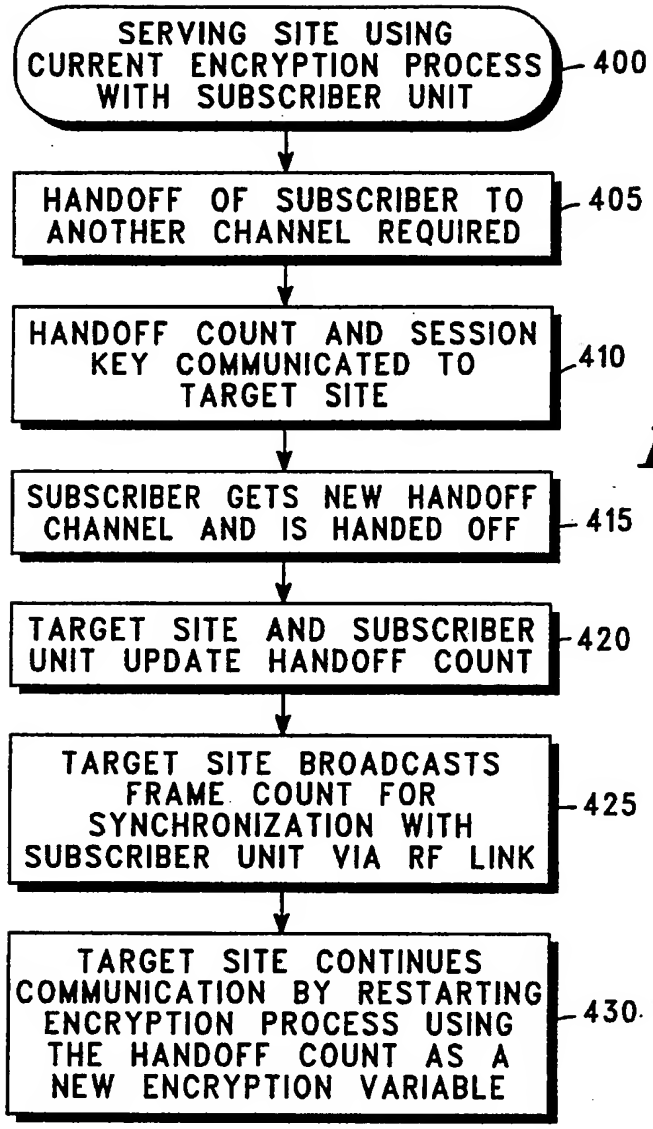
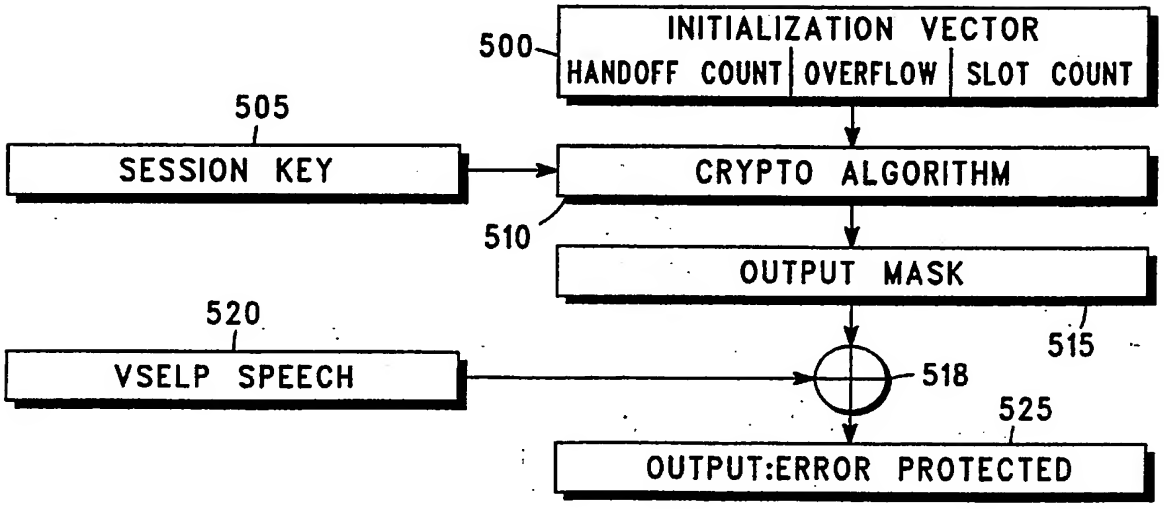

SERVING SITE USING CURRENT ENCRYPTION PROCESS WITH SUBSCRIBER UNIT
400
HANDOFF OF SUBSCRIBER TO ANOTHER CHANNEL REQUIRED
405
HANDOFF COUNT AND SESSION KEY COMMUNICATED TO TARGET SITE
410
SUBSCRIBER GETS NEW HANDOFF CHANNEL AND IS HANDED OFF
415
TARGET SITE AND SUBSCRIBER UNIT UPDATE HANDOFF COUNT
420
TARGET SITE BROADCASTS FRAME COUNT FOR SYNCHRONIZATION WITH SUBSCRIBER UNIT VIA RF LINK
425
TARGET SITE CONTINUES COMMUNICATION BY RESTARTING ENCRYPTION PROCESS USING THE HANDOFF COUNT AS A NEW ENCRYPTION VARIABLE
430

FIG.4

FIG.5


500
INITIALIZATION VECTOR
HANDOFF COUNT
OVERFLOW
SLOT COUNT
505
SESSION KEY
CRYPTO ALGORITHM
510
OUTPUT MASK
515
520
VSELP SPEECH
518
525
OUTPUT:ERROR PROTECTED

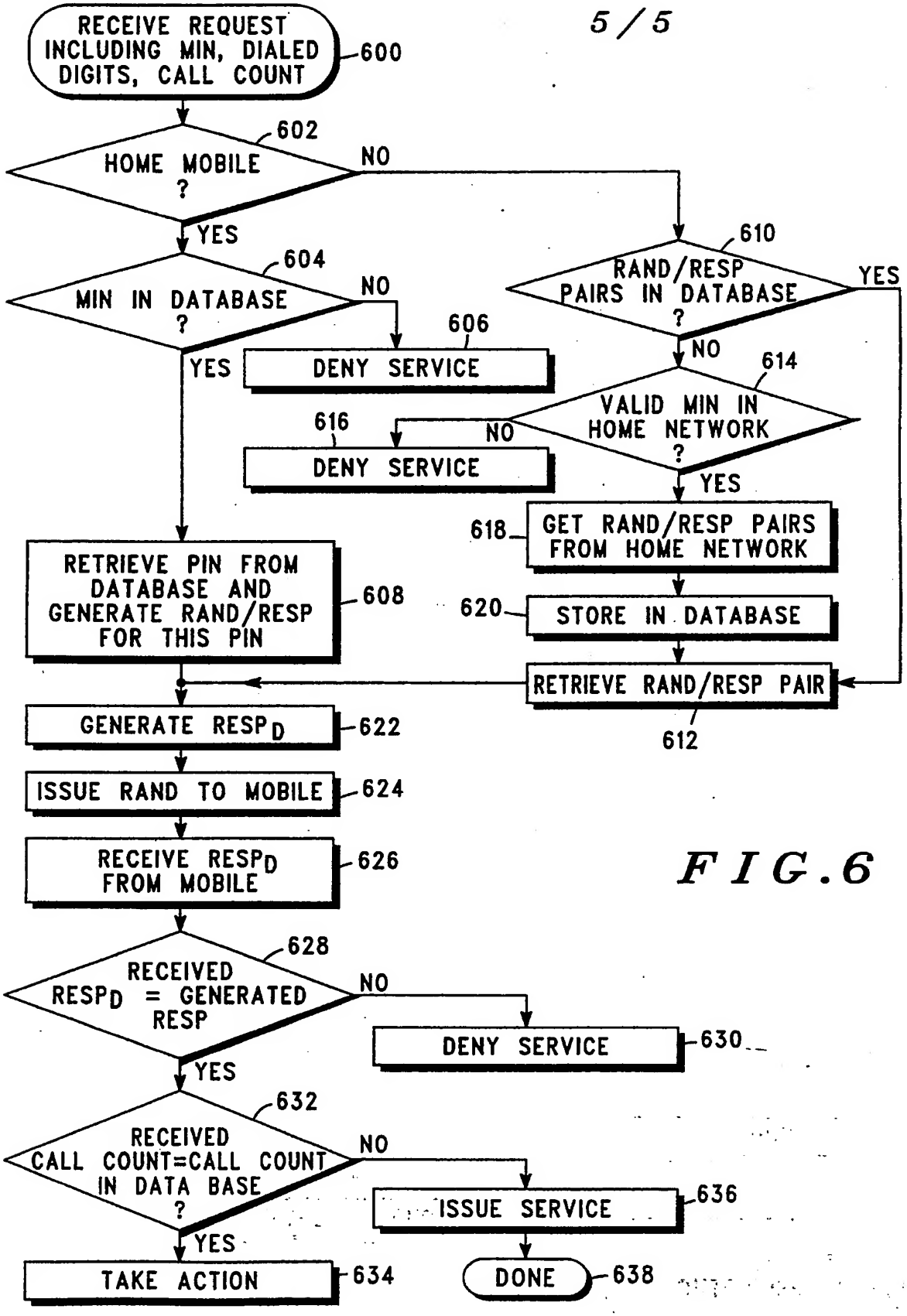

RECEIVE REQUEST INCLUDING MIN, DIALED DIGITS, CALL COUNT
600
HOME MOBILE ?
602
NO
YES
MIN IN DATABASE ?
604
NO
YES
DENY SERVICE
606
RAND/RESP PAIRS IN DATABASE ?
610
YES
NO
VALID MIN IN HOME NETWORK ?
614
NO
DENY SERVICE
616
YES
GET RAND/RESP PAIRS FROM HOME NETWORK
618
STORE IN DATABASE
620
RETRIEVE RAND/RESP PAIR
612
RETRIEVE PIN FROM DATABASE AND GENERATE RAND/RESP FOR THIS PIN
608
GENERATE RESP$_D$
622
ISSUE RAND TO MOBILE
624
RECEIVE RESP$_D$ FROM MOBILE
626
RECEIVED RESP$_D$ = GENERATED RESP
628
NO
DENY SERVICE
630
YES
RECEIVED CALL COUNT=CALL COUNT IN DATA BASE ?
632
NO
ISSUE SERVICE
636
YES
TAKE ACTION
634
DONE
638

FIG. 6

INTERNATIONAL SEARCH REPORT

International Application No. PCT/US91/04970

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [6]

According to International Patent Classification (IPC) or to both National Classification and IPC

IPC (5); H04 Q 7/00
U.S.Cl, 340/825. 340

II. FIELDS SEARCHED

Minimum Documentation Searched [7]

Classification System	Classification Symbols
US	340/825.340, 825.33, 825.69, 825.72, 825.3, 825.31 379/59, 62,63

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched [8]

III. DOCUMENTS CONSIDERED TO BE RELEVANT [9]

Category *	Citation of Document, [11] with indication, where appropriate, of the relevant passages [12]	Relevant to Claim No. [13]
Y	US,A, 4315101 (ATALLA) 09 February 1982 Note abstract; Fig. 1A, 5; col. 2, lines 25-40; col. 3, lines 45-70; as well as entire document.	1-10
Y	US,A 4814741 (HONGO et al.) 21 March 1989 See col. 2, lines 60-70; col. 3, lines 56-70; col. 4, lines 20-31; and entire document	1-10
Y	US,A, 4023012 (ANO et al.) 10 May 1977 See entire document	1-10

* Special categories of cited documents: [10]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
21 August 1991	17 SEP 1991
International Searching Authority	**Signature of Authorized Officer**
ISA/US	Peter Weissman

Form PCT/ISA/210 (second sheet) (Rev. 11-87)